California Department of Corrections and Rehabilitation /
California Prison Health Care Services

Directory Cohabitation Governance

Version 1.3

August 21, 2009

Revision History

Date	Version	Description	Author
03/June/09	1.00	Initial draft	Kim May
04/June/09	1.01	Minor revisions from EMC	Eli Hill
06/June/09	1.02	Revisions from Discussions with Governance Team	Kim May
22/June/09	1.03	Added boards and panels structure, workflow and cost allocation sections.	Kim May
18/August/09	1.04	Minor edits, page numbers, and captions.	Nancy R. Raley
19/August/09	1.1	Minor edits.	Kim May
20/August/09	1.2	Minor edits.	Nancy R. Raley
21/August/09	1.3	Minor edits, spell check, updated header, added date to file name, minor formatting, removed draft watermark.	Nancy R. Raley

Table of Contents

Executive Summary 1

1. Introduction 1
1.1 Purpose 1
1.2 Scope and Layout 1

2. Basic Governance Structure 1
2.1 Governance Framework 1
2.2 Agency/Department Relationship 2
2.3 Boards and Panels 2
2.3.1 AD Governance Team 3
2.3.2 AD Change Control Board 4
2.3.3 Technical Working Group 4
2.4 Change Control Process 4
2.4.1 Change Control Process Workflow 4
2.4.2 Agenda-Based Change Request Vetting 5
2.4.3 Change Request Form 5
2.4.4 Change Request Risk Classification 6
2.4.5 Change Request Impact Assessment 6
2.4.6 Change Request Approval and Communication Requirements 7
2.5 Conflict Resolution/Escalation 7

3. Administrative Rights/Roles 7
3.1 Enterprise/Domain Administrators 7
3.2 Root/Department OU Administrators 7
3.3 Unit Level Delegates 8
3.4 Information Technology Service Desk 8

4. Cost Allocation 8

5. Scorecard 8
5.1 Scorecard Purpose 8
5.2 Scorecard Example 8
5.3 The AD Scorecard 9

Appendix A: Change Control Form 11

Appendix B: AD Services - What goes to Change Control? 13

Appendix C: Role and Resource Assignments 14

Executive Summary

The California Prison Health Care Receivership (CPR) was mandated to improve medical care in the California Department of Corrections and Rehabilitation (CDCR). Once improvements have been made, the receivership will return control of prison health care services to the state. In the context of information technology, sufficient improvements must be achieved in keeping with providing a constitutional level of care to California's inmates.

There is an initiative by the Office of the Chief Information Officer (OCIO) to provide centralized identity management guiding consolidation and a standardized governance model for all agencies at the state. In this context, the departments at the CDCR agency, including CDCR, California Prison Health Care Services (CPHCS), and the Prison Industry Authority (PIA), will cohabitate in the same directory infrastructure. At the department level, CDCR and CPHCS are currently cohabitating in the same directory; PIA will be integrated later.

This document provides an abbreviated governance framework for the directory services for CDCR and CPHCS to meet the short-term goals of accommodating CPHCS' application projects, including Dictation and Transcription (D&T) and Clinical Data Repository (CDR).

1. Introduction

1.1 Purpose

The purpose of this document is to identify briefly the governance approach for managing the initial directory cohabitation efforts of CDCR, CPHCS, and PIA. It will also lay out how these organizations will interface with the Office of Technology Service (OTech)-hosted consolidated California Directory Services.

1.2 Scope and Layout

This document provides only a short-term governance approach to meet the immediate needs of the Active Directory (AD) cohabitation efforts to provide stable and continued operations. The processes contained within this document address AD changes necessary to support the CDCR and CPHCS integration with the statewide AD but focus solely on short-term needs. Longer-term AD governance plans will be established with more robust and scalable processes to support the maintenance and operation of the integrated AD solution.

2. Basic Governance Structure

This section identifies the framework entities and personnel impacted by the AD governance methods described in this document.

2.1 Governance Framework

A basic governance framework has been established. This framework could easily be extended, but will likely be impacted or replaced by ongoing governance and enterprise architecture efforts being conducted in the State of California.

For the short-term needs of this effort, this governance structure will be limited to the operational governance-level activities highlighted by the red outline in Figure 1. The processes and activities identified in this document will be defined as required to mitigate risk, optimize interoperability, and provide for stable operation of the consolidated cohabitation AD structure.

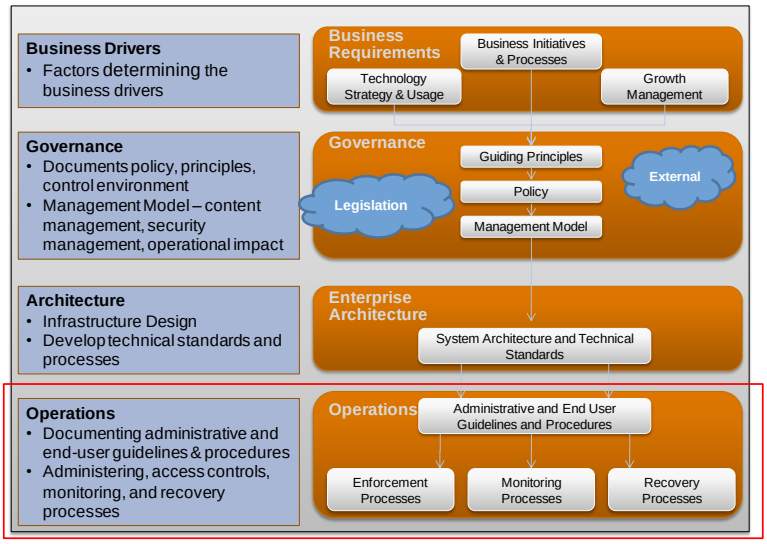


Figure 1 Basic Governance Framework

2.2 Agency/Department Relationship

Figure 2 depicts the governance relationship between the Office of Technology Services (OTech), CDCR, and the department-level IT structures.

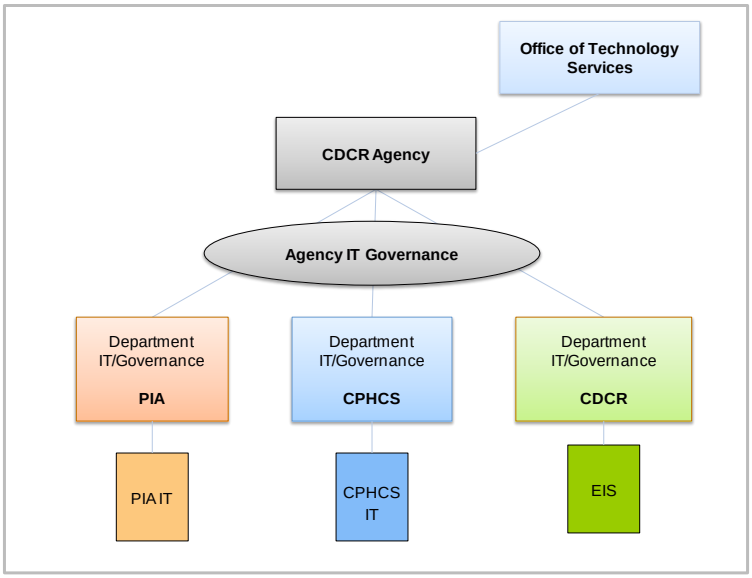


Figure 2 Agency/Department AD Governance Relationship

2.3 Boards and Panels

The following sections outline the board and panel structure specific to the cohabitation AD structure. Figure 3 provides a high-level view of the relationships and roles of the governing bodies. Information that is more detailed is contained in the sections below.

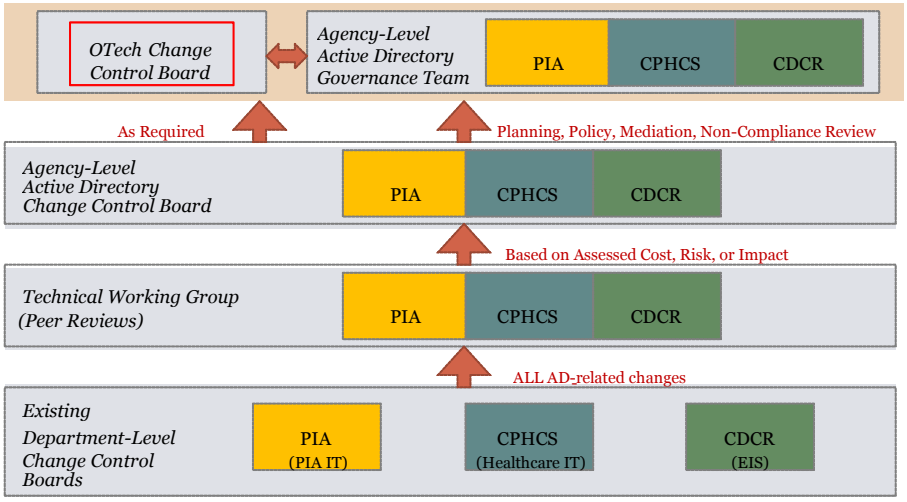


Figure 3 Boards and Panel Structure

2.3.1 AD Governance Team

The AD Governance Team (ADGT) will function at the CDCR agency-level and be representative of agency-wide interests. This executive-level team includes members from CDCR, CPHCS, and PIA. Initial role and resource assignments for the ADGT appear in *Appendix C: Role and Resource Assignments.*

The duties of the AD Governance Team are:

- Identification and approval of objectives, business drivers, and requirements;
- AD policy creation or change;
- AD policy non-compliance review;
- Mediation in the case of any technical disputes between groups; and
- Approval of major architectural change.

The ADGT will rely on their technical staff for guidance, help in prioritizing any changes to the AD environment, as well as to work with technical resources and departmental computing units to help integrate AD aware applications. The ADGT will also be responsible for reviewing policies regarding the computing environment on an ongoing basis in order to ensure that they are reflective of changes that may occur over the course of time. Future versions of this document that focus on mid-term and long-term needs will contain additional information, such as triggers, review intervals, and processes.

The ADGT will meet initially once a month to review any requests, mitigate any disputes, and perform any other administrative functions that may be deemed necessary. During the initial cohabitation period, the ADGT may be required to meet more frequently. Following the initial phases of process change and extension to shared statewide services, the ADGT will meet at an appropriate regularly scheduled interval.

Any ADGT member may request a non-scheduled ADGT meeting if the conditions warrant. The ADGT member requesting the non-scheduled meeting is responsible for coordinating the meeting time and location with the other ADGT members.

ADGT decisions require participation from CDCR, CPHCS, and PIA. To address situations in which action must be taken quickly, it is important that the ADGT is consistently able to meet on an ad hoc basis. Therefore, it is essential that the ADGT members designate and empower one or more *alternate* resources to act in the place of the primary member, when the primary member is unavailable. Initial role and resource assignments for the ADGT appear in *Appendix C: Role and Resource Assignments*.

The ADGT or their representative will be responsible for creating and archiving minutes of all ADGT meetings. The time and location of these meetings is to be determined.

2.3.2 AD Change Control Board

An Active Directory Change Control Board (ADCCB) will be established for the purpose of reviewing and approving high- and medium- risk and moderate to severe impact Change Requests (CR), after the CRs have been reviewed and prioritized by representatives of the Technical Working Group. Representatives or their delegates from each department will be required at the ADCCB to approve CRs prior to implementation of changes to the cohabitated AD structure. Roles and resource assignments for the ADCCB appear in *Appendix C: Role and Resource Assignments*.

At times, it may be necessary to include Office of Technology Services (OTech) representation in ADCCB processes. In particular, this should occur when a CR affects the California Directory Services or falls outside of the Office of Technology Services (OTech) change control process. Future versions of this document that focus on mid-term and long-term needs will contain additional information about OTech's role in AD governance.

An opportunity exists to extend the existing CDCR CCB to include ADCCB agenda items. Careful consideration is being given as to when this expansion could possibly be put into place, but it is not considered an immediate option.

Any ADCCB member may request a non-scheduled ADCCB meeting in a situation where a change must be implemented prior to the next ADCCB meeting. The ADCCB member requesting the non-scheduled meeting is responsible for coordinating the meeting time and location with the other ADCCB members.

ADCCB decisions require participation from CDCR, CPHCS, and PIA. To address emergency situations, where action must be taken immediately, it is important that the ADCCB is consistently able to meet on an ad hoc basis. Therefore, it is essential that the ADCCB members designate and empower one or more *alternate* resources to act in the place of the primary member, when the primary member is unavailable.

Provisions will be made by the members of the ADCCB on a case-by-case basis for addressing CRs containing confidential information. This provision could be as simple as holding the confidential agenda item as the last reviewed and reducing the meeting attendance to accommodate the appropriate level of confidentiality.

Some form of the initial ADCCB will be established immediately. It was discussed and agreed upon by CDCR and CPHCS that until a more formal process is rolled out, that advanced email notification and response of approval would be acceptable in the immediate term. Until a more formal process is implemented, the members of the ADCCB or their representative will be responsible for creating and archiving these email responses.

It is anticipated that in the longer-term, the ADCCB will meet weekly at a regular and ongoing interval. The time and location of these meetings is to be determined.

2.3.3 Technical Working Group

A working-level Technical Peer Review process will be put into place to review all change requests and confirm their risk and impact assessment levels. This working group will contain designated representatives from CDCR, CPHCS, and PIA. This team can recommend courtesy notification via email to the AD cohabitation partners should a change not warrant their review but be worthy of attention on an informational basis.

Technical analysis of CRs requires participation from CDCR, CPHCS, and PIA. To address situations in which action must be taken quickly, it is important that the technical resources are consistently available to evaluate CRs. Therefore, it is important that sufficient primary and backup resources be identified to address CR reviews.

2.4 Change Control Process

The section below includes information on the change control process to be used for risk mitigation and communication of change for AD cohabitation. T he process developed here will continue to be refined and developed as the operational scenarios mature. This process is intended for the short-term effort only.

2.4.1 Change Control Process Workflow

The change control sample workflow in Figure 4 provides a bottom up view of the possible paths for change control and approval, using department change control processes as the point of origination. Future versions of this document that focus on mid-term and long-term needs will address changes that are initiated from other sources,

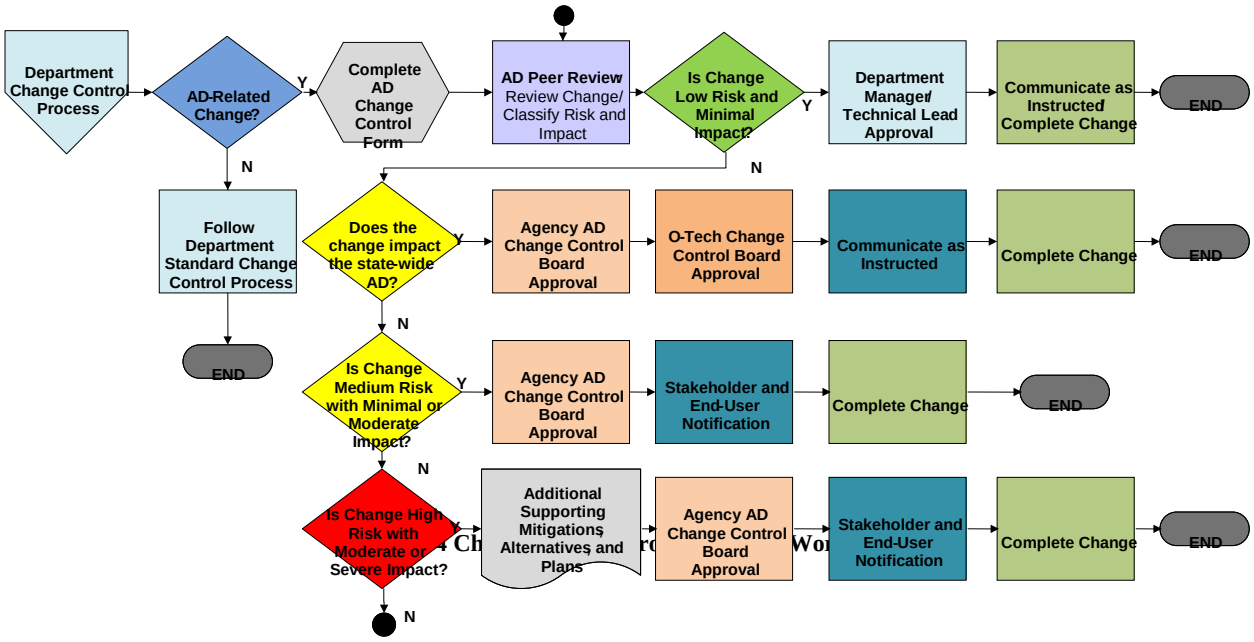
such as OTech.

Assuming that the majority of changes are going to be initiated at the department level, the change control process identifies AD-related changes and steers them toward completing the appropriate change control form. Once the form is completed, it is peer reviewed where is classified for risk and expected impact based on the tables contained in Sections 2.4.4 and 2.4.5. If the change is rated as both low risk and minimal impact, the change can be approved by the Department Manager or Technical Lead. The Department Manager or Technical Lead will also dictate the communication plan prior to the change being completed. All non-AD changes will continue to follow the standard department-level change control process.

If the AD change requested is determined to have a statewide impact, then the change will proceed to the agency-level ADCCB for approval and then to the OTech Change Control Board for approval. Again, communication will be dictated by one or both of those Boards as required prior to the change being completed.

If the requested AD change is classified to be of medium risk with minimal or moderate impact, approval will be made at the agency ADCDB. Medium risk changes also require stakeholder and end-user notification prior to the change being completed. OTech is considered a stakeholder in this scenario.

High Risk changes with moderate or severe impacts will require additional supporting documentation, such as risk analysis, mitigating actions, alternatives reviewed, and possibly full-blown coordinated plans prior to approval. High Risk changes can be approved by the agency-level ADCCB. They will require stakeholder and end-user notification prior to the change being completed. OTech is considered a stakeholder in this scenario.



2.4.2 Agenda-Based Change Request Vetting

An advance copy of the ADCCB agenda will be provided to an established ADCCB distribution list at least four business days prior to the scheduled meeting to ensure that the members have the appropriate time to review the CRs and to ensure appropriate supporting representation.

2.4.3 Change Request Form

A sample CR form has been included in *Appendix A: Change Control Form*, although an existing form may be used if it is part of an established process. The change request form needs to include an assessment of the anticipated risks and impacts.

2.4.4 Change Request Risk Classification

The following matrix includes a standardized approach to risk assessment as related to system change management requests. All CRs classified as a high or medium risk are reviewed by the established ADCCB.

Table 1 Risk Levels

Risk Level	Risk Description
High	Change will possibly result in: • the loss of hardware, software or critical data • OR loss of system availability outside of the scheduled window • OR significant financial impact • OR risk of regulatory non-compliance or violation • OR impacts to the requested change are unknown.
Medium	Change will possibly result in: • measureable, but recoverable impact to, or loss of, H/W, S/W or data • OR complete loss of system availability for a scheduled period of time • OR moderate slip to project critical path that will cause a delay in project deliverables • OR cost impacts within an expected contingency budget • OR moderate impacts on system supportability • OR impact to regulatory compliance.
Low	Change will possibly result in: • No detectable impact to, or loss of, H/W, S/W or data • OR minimal loss of productivity or schedule impact • OR no potential cost impact. • OR frequently completed and routine tasks requiring no system interruptions.

2.4.5 Change Request Impact Assessment

Impact is determined by the potential negative consequence that a CR could have on customers. Impact analysis should be based on the worst-case scenario for a competent administrator and include any negative consequences from successfully performing the change.

Table 2 Risk Impacts

Impact Type	Impact Description
Severe	• Vital business function • Major systems or impacts multiple customers • Public impact • Difficult to recover within scheduled window • No backout possible • No redundant resource
Moderate	• Vital business function • Outside the maintenance window • Potential public impact • Multiple components with interdependencies • Backout/restore without significant difficulty • No redundant resource • ENews article required.
Minimal	• Off-hours when not in use or maintenance windows • No public impact • Simple backout/restore • Redundant resource

2.4.6 Change Request Approval and Communication Requirements

The approval process and communication requirements based on identified risk level are outlined in Table 3.

Table 3 Risk Approval & Communication

Risk Level	Impact Assessment	Approval Process	Communication Requirements
High	Moderate or Severe	Completed form and appropriate supporting documentation must be reviewed and approved by the ADCCB.	Executive Management (information only), Stakeholder, and User advanced notification (impacts and risk mitigation as required) unless otherwise approved by ADCCB.
Medium	Moderate or Minimal	Completed form must be reviewed and approved by the ADCCB.	Stakeholder and User notification as required (impacts and risk mitigation as required).
Low	Minimal	Appropriate Manager or Technical Lead Signatures.	As instructed by Manager or Technical Lead

2.5 Conflict Resolution/Escalation

Should a situation warrant, escalation above the CDCR agency could be made to the Agency Information Officer (AIO) level for conflict resolution. Future versions of this document that focus on mid-term and long-term needs will contain additional information regarding escalation.

3. Administrative Rights/Roles

The sections below outline the anticipated administrative rights and roles by administration type. Best practices are to provide the minimum level of access required to perform a function successfully and to minimize the number of administrators performing directory functions where possible.

3.1 Enterprise/Domain Administrators

Enterprise/Domain Administrators will have permission to: Change Schema, Create Trusts, Add Domain Controllers, Add Directory Services (DHCP, DNS, WINS, CA), perform Structural Changes, update Site Topology, Author and Apply Domain Level Group Policies.

A custodial group will be established with one Enterprise/Domain Administrator each for CDCR, CPHCS, and PIA and one backup administrator/apprentice identified.

A process will be established to identify and ensure an administrator's level of competency prior to granting this level of access.

A process will be developed to manage service-type accounts that require Domain Administration-type privileged access. Ideally, no applications will be granted this type of access as alternative solutions will be implemented.

3.2 Root/Department OU Administrators

Root/Department Organization Unit (OU) Administrators will be delegated the authority to add/modify/delete objects (e.g., computers, users, groups, and contacts), manage user-level Exchange attributes delegate per department, and to add/modify/delete sub-level OU's.

Upon implementation of the Microsoft Desktop Optimization Pack (MDOP) Advanced Group Policy Management Tool, Root/Department OU Administrators will be able to manage Group Policy Objects within their OU structure.

A process will be established to identify and classify an administrator's level of competency prior to granting this level of access.

The Root/Department OU Administrator role is to be established and approved at the appropriate department level.

3.3 Unit Level Delegates

Local IT staff and other unit level delegates will be provided delegation of OU functions similar to that of a Root/Department OU Administrator except the Group Policy functions and OU manipulation. Unit Level Delegates will be established and approved at the department level.

3.4 Information Technology Service Desk

The Verizon-provided Help Desk Support through the Information Technology Service Desk (ITSD) will be granted the ability to Add/Modify/Delete/Move/Change Memberships for all object types and Exchange attributes.

4. Cost Allocation

Currently, CDCR as an Agency and its associated departments do not have a charge-back model for allocation of costs. Cost sharing for collaborative efforts is done on a case-by-case basis with each of the affected parties contributing when and where they can. Thus, costs are not based on usage or necessarily shared evenly.

If any of the parties participating in a shared workstream or collaborative effort do not feel that AD-related costs are being shared fairly, they should escalate this matter to the ADGT for resolution or further escalation to the appropriate AIO.

5. Scorecard

The section below contains information on the development and tracking of service-related metrics in an AD scorecard format.

5.1 Scorecard Purpose

The AD scorecard is intended to provide unbiased, fact-based metrics to indicate whether the cohabitation efforts are successful, as well as identify areas needing mitigating efforts.

5.2 Scorecard Example

Figure 5 is an example scorecard showing a format that will be useful in capturing and reporting metrics for the first six months of this initiative. This is a simple example generated manually.

IM Service Level Agreement

METRIC	Goal/ Desc.	FY07	FY08	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	Jul
Incident resolution	Priority 2	32%	29.1%	44%	57%	44%	45%	41%	60%				
	Compliance	36	48	20	16	15	22	17	26				
	Total	91	169	45	28	34	49	41	43				
	Priority 3	54%	70.9%	69%	74%	77%	75%	70%	75%				
	Compliance	11332	14296	1309	960	930	1253	1155	1289				
	Total	15882	20163	1909	1303	1265	1721	1639	1713				
Request For Service 1 (RFS1) Closed < 7 days	Green=80% Red<70%	93.6%	93.6%	94%	93%	94%	93%	92%	94%				
	# < 7 days	6363	6340	557	451	219	318	280	272				
	Total Calls	6814	6767	590	483	234	342	304	290				
Request For Service 2 (RFS2) Closed < 7 days	Green=80% Red<70%	82.9%	83.4%	87.4%	81.9%	77%	82.1%	75%	84.8%				
	# < 7 days	5812	3914	285	163	162	280	226	263				
	Total Calls	6982	4680	326	199	211	341	301	310				
Telephone Service Requests < 3 Bus. Day	95.0%	97.9%	98.5%	100.00%	97.83%	93.75%	96.92%	100.00%	95.74%				
Telephone Repairs < 1 Business Day	95.0%	96.2%	96.8%	93.10%	100%	94.12%	94.12%	99.84%	96.55%				

EXAMPLE

Figure 5 Service Level Example

Ideally, as the process matures, an ITIL service-based approach can be developed to track and report upon service-level metrics. Development of these efforts often includes a great deal of planning, as well as toolsets to automate the accumulation of information. In an ITIL-type scorecard, the services would be tracked in the following manner:

- Active Directory
  - Availability 99%
  - Changes 2
  - Problems 0
  - Incident Reports 25
  - Number of Users 300
  - Inquiries 100
  - Access requests 10
- Network
  - Availability 99%
  - Changes 5
  - Problems 1
  - Incident Reports 50
  - Number of Users 200
  - Inquiries 100
  - Access requests 5

5.3 The AD Scorecard

Figure 6 depicts an initial draft of an AD Scorecard displaying the types of information that may be collected if metrics are available. This scorecard will need to be refined and defined as discussed below.

Metric	Goal/Description	Jun	Jul	Aug	Sept	Oct	Nov
AD Availability	**99.9% (Uptime less Scheduled Maintenance)**						
	Possible Hours in Month						
	Accumulated Maintenance Hours						
	Unplanned Outage Hours						
	Total						
AD Incident Reports	**<1 – Green, 1-3 – Yellow, 3+ - Red**						
Server Incidents							
Corruption							
Object Recovery							
Enterprise Responsiveness	**Approved CR Closure Timeframes**						
	Qty in less than 1 hour						
	Qty in less than 24 hours						
	Qty in over 24 hours						
Number of Emergency Changes	**<1 – Green, 1-3 – Yellow, 3+ - Red**						
Security Related Changes	**<1 – Green, 1-3 – Yellow, 3+ - Red**						
Firewall	TBD						
Network	TBD						

Figure 6 Sample AD Scorecard

A best practice related to metrics collection is to collect new measures for six months prior to establishing a goal or description. In this case, AD is not new to any of the environments and six months is the only established collection time. Agreement by the affected parties on both the metrics and the goal/description initially will be required. It is important to note, that the goals and metrics can be adjusted as required and approved by the ADGT.

In addition, a plan will need to be developed for collecting the metrics. The following items need to be identified for each metric:

- Who
  - Who is responsible for data collection and who receives reports? (Best if standardized)
- What
  - What data metrics are collected?
  - What formulas are used? (e.g. Availability)
  - What consequences exist for not meeting specified service levels?
- Where
  - How many entities provide data? Where is it coming from?
- When
  - Frequency of data collection?
  - Frequency of reporting? Age of data? Response time requirements?
- Why
  - Why are we gathering information and for what is it being used?
- How
  - How is data collected and reported? Automated/manual (Method for consistent capture)

Two main cautions regarding data collection are: 1) be careful what you measure – people will master what they will be measure on; and 2) be careful not to over-engineer the process.

Appendix A: Change Control Form

Future versions of this document that focus on mid-term and long-term needs will contain an updated Change request Form to incorporate approval signatures, one-time or ongoing resource clarifications, "manager assigned" resource name, and additional data about requested changes.

Change Control Form

TITLE:
REQUESTING DEPARTMENT:

For Change Management Use:	**REQUESTED TIME SCHEDULE**			
Change Request #:	**Requested Date(s):**			**Requested Time(s):** **From:** **To:**
Date Received:	**Within Maintenance Window?**	Yes ☐	No ☐	**Estimated Time to Complete:**
Date Closed:	**Is this an Outage?**	Yes ☐	No ☐	**Outage Time:** **From:** **To:**

REQUESTOR INFORMATION		
Name:	**Phone:**	**Pager:**
Manager:	**Phone:**	**Pager:**

CHANGE TYPE				
Software:	New ☐	Upgrade ☐	Fix ☐	**Other (explain):**
Hardware:	New ☐	Upgrade ☐	Fix ☐	**Other (explain):**
OS:	New ☐	Upgrade ☐	Fix ☐	**Other (explain):**

CHANGE INFORMATION			
Description of Change:			
Reason for Change:			
Platform: **Server:**			
System Reboot Required?	Yes ☐ No ☐	**Will Change Affect Users?**	No ☐ Yes Please explain effect in comments section. Without explanation this may cause a delay in processing request.
Risk Assessment	☐ High ☐ Medium ☐ Low (See Risk Classification Matrix) Explain expected impacts:		

DISASTER RECOVERY PLAN	
Disaster Recovery Plan?	Not Required ☐ No ☐ Yes ☐ (If Yes, please describe below)

IMPLEMENTATION PLAN	
Implementation Procedure:	
Verification Procedure:	
Backout Procedure:	

Change Control Form (page 2)

IMPLEMENTATION SUPPORT / APPLICATION SUPPORT			
Name	**Phone**	**Alternate Number**	**Department**

CHANGE PRIORITY			
Type	**Definition**	**Immediate Notification**	**Lead Time**
Emergency ☐	Severe disruption to mission critical systems/applications.	Upon approval, inform ChangeControl immediately.	Upon approval.
Normal ☐	Planned / Scheduled changes.	Normal notification process.	1 week prior to maintenance window.

COMMENTS

Appendix B: AD Services - What goes to Change Control?

- All Medium and High Risk Activities
- Anything that impacts the enterprise level
- Change Schema
- Create Trusts
- Adding/Removing/Rebooting Hub Site Domain Controllers
- Adding/Modifying/Deleting Directory Services (DHCP, DNS, WINS, CA)
- Root OU Structural Changes
- Site Topology Changes
- Domain Level Group Policies Changes
- Domain Controller Policy
- Changes to Standard Domain Controller Build Procedures
- Elevation of privileges to domain schema level
- Adding Privileges to Quest Change Auditor

Appendix C: Role and Resource Assignments

Role and resource assignments for governance of the cohabitation AD environment appear in Table 4. These assignments may change over time. An updated list of assignments for AD governance will appear in a future version of this document.

Table 4 AD Governance Role Assignments

Board or Panel	Description	Assigned Roles	Assigned Resources
Active Directory Governance Team (ADGT)	An agency-level body responsible for approval of objectives, business, drivers, and requirements, AD policy, non-compliance review, mediation. Also responsible for approval of Change Requests for major architectural change.	Primary members are the AIO, CIO, or Deputy CIO. Additional membership is to be determined.	Primary members are: - Elbert Lawrence, CDCR, Deputy CIO - Liana Bailey-Crimmins, CPHCS, Deputy CIO - Sheila Howell, PIA, CIO Alternate (backup designee) members are to be determined.
Active Directory Change Control Board (ADCCB)	Governing body, made up of representatives from the partners in the cohabitation AD environment: CDCR, CPHCS, and PIA. This body meets regularly to review and disposition (approve/disapprove) high and medium risk and moderate to severe impact Change Requests affecting the cohabitation AD environment.	Primary members are the CIO or Deputy CIO Additional membership is to be determined.	Primary members are: - Elbert Lawrence, CDCR, Deputy CIO - Liana Bailey-Crimmins, CPHCS, Deputy CIO - Sheila Howell, PIA, CIO Alternate (backup designee) members are to be determined.
AD Technical Working Group	Analytical resources group, made up of technical personnel from the partners in the cohabitation AD environment: CDCR, CPHCS, and PIA. This group is responsible for reviewing and prioritizing Change Requests according to risk and impact in the context of cohabitation AD environment.	To be determined	To be determined
OTech Change Control Board	Governing body established by the Office of Technology Services, responsible for approval of Change Requests affecting the California Directory Services (statewide AD).	To be determined	To be determined